UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,696	09/12/2003	David D. Brandt	03AB014C/ALBRP303USC	7375

7590 08/02/2010

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
08/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,696	BRANDT ET AL.	
	Examiner	Art Unit	
	RONALD BAUM	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,12-17,19-21,23,25,30,41 and 45-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,12-17,19-21,23,25,30,41 and 45-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 21 May 2010.

2. Claims 1-9, 12-17, 19-21, 23, 25, 30, 41 and 45-52 are pending for examination.

3. Claims 1-9, 12-17, 19-21, 23, 25, 30, 41 and 45-52 are rejected.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 21 May 2010 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9, 12-17, 19-21, 23, 25, 30, 41 and 45-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swiler et al, U.S. Patent 7,013,395 B1 in view of Townsend, U.S. Patent 6,374,358 B1, and further in view of Godwind, U.S. Patent Publication US 2004/0059920 A1.

Prior Art's Broad Disclosure vs. Preferred Embodiments

As concerning the scope of applicability of cited references used in any art rejections below, as per MPEP § 2123, subsection R.5. Rejection Over Prior Art's Broad Disclosure Instead of Preferred Embodiments:

I. PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also > Upsher-Smith Labs. v. Pamlab, LLC, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005)(reference disclosing optional inclusion of a particular component teaches compositions that both do and do not contain that component);< Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention.). >See also MPEP § 2131.05 and § 2145, subsection X.D., which discuss prior art that teaches away from the claimed invention in the context of anticipation and obviousness, respectively.<

II. NONPREFERRED AND ALTERNATIVE EMBODIMENTS CONSTITUTE PRIOR ART
Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed...." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).

Swiler et al *generally* teaches and suggests (i.e., Abstract, figures 1-2 and associated descriptions in general) the limitations set forth in the claims below (e.g., claim 1), as modified by the Townsend and Godwin teachings as further described below.

5. As per claim 1; "A security analysis tool for an automation system having a controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising:

a learning component that

monitors the communication of data

associated with the I/O table

during a training period and

generates a learned pattern of communication [*figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of* ***factory assets****, inclusive of system information acquisition ('... a learning component ... monitors the communication of data ... during a training period ') as part of the monitoring/scanning of communications to/from the network computer, whereas for the case of factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of - at the very least - programmable logic controllers of which industrial controllers are an associated architecture), such that industrial controllers running standard operating systems (e.g., col. 2,lines 3-67; UNIX, Windows, etc.,) use I/O data structures to at least deal with interface processing (e.g., I/O tables involved in port communications (i.e., hardware driver support of serial ports, parallel ports, USB ports, and communications ports that deal with both a port physical network address and associated application involved during packet communications generally; '... I/O device ... I/O table ...') processing, etc.,), clearly dealing with Intranet/Internet access patterns insofar as network security per se is concerned) and attack template (i.e., a model; '... generates a learned pattern of communication ...') information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration*

changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]; and

an analyzer component that

monitors data traffic

subsequent to the training period and

generates one or more security outputs

if a current pattern of the data traffic deviates

from the learned pattern

in excess of the acceptable deviation [*figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs; '... generates one or more security outputs ...') used to evaluate (i.e., graphed output information)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (relative to the learned/acquired model/template; ' ... from the learned pattern ...'), clearly encompassing the claimed limitations as broadly interpreted by the examiner.*],

the one or more security outputs including

at least one output that alters the data traffic between

the controller and

the at least one I/O device [*Townsend and further in view of Godwind below*].

It is noted that Swiler et al, does not disclose the specific type of action taken upon vulnerability assessment results determination, insofar as additional security components are required (i.e., installation) upon a vulnerability or detected security problem so determined. However, the examiner asserts that it would have been obvious to one ordinary skill in the art at the time the invention was made for the adaptive countermeasure selection method/apparatus of Townsend to be combined with the validation component vulnerability assessment results of Swiler et al, insofar as the Swiler et al teaching of a computer system analysis tool ***requiring a responding mechanism to make use of the analysis tool output*** (i.e., the Townsend countermeasure selection method/apparatus installation countermeasures aspects, col. 3,lines 17-33, col. 7,lines 33-65), and would be in itself an obvious intended use. However, Townsend does not explicitly deal with the automated aspect of the countermeasures. Godwin teaches of using an automated tool to automatically (e.g., Godwin, ¶0019-0022, 0031) adjust security parameters (i.e., again, as a result of the Townsend countermeasure selection method/apparatus installation countermeasures aspects) for ***online*** storage systems (e.g., the industrial controller storage functionality per se in the industrial control/enterprise environment), encompassing communications control – broadly – insofar as access control to a network storage entity constitutes output control correction relative to a prior network communications state. Further, Godwind teaches the checking/editing/updating/etc., of security settings *manually* (e.g., Godwin,

¶0019-0022, 0031, 0073-0136, inclusive of bounds limitations on the parameter determination updating, etc.,) for network processing computers/processing elements, upon discerning via a security policy/rules criteria analysis that said security settings require said editing/updating/etc., is costly and error prone, and can be enhanced via automating the process.

Such motivation to combine would clearly be an obvious requirement, insofar as using the validation component vulnerability assessment results of Swiler et al to require the vulnerability results to be utilized as a practical business aspect of requiring the vulnerability assessment in the first place (e.g., Townsend business concerns requiring countermeasures, col. 3,lines 1-50), as implemented in an automated manor because of the costly and error prone checking/editing/updating/etc., of security settings *manually* for network processing computers/processing elements, upon discerning via a security policy/rules criteria analysis that said security settings require said editing/updating/etc.

A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987).

As per claim 12, this claim is the method claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 16, this claim is the means plus function claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 17, this claim is an apparatus (a security validation system) claim variation for the (security analysis tool) system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, insofar as the claim 1 tool results in effective security validation as a function of the security output aspects of the claims.

As per claim 30, this claim is the means plus function claim for the system claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

6. Claim 2 ***additionally recites*** the limitation that; "The tool of claim 1, further comprising an interface component

that generates a description of

one or more industrial controllers in the automation system".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component) computer system/network configuration/topology (i.e., description of factory assets - clearly ' industrial controllers in the automation system ') and attack template (i.e., model; '… generates a description of …') information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 ***additionally recites*** the limitation that; "The tool of claim 2, wherein at least one of the interface component or the analyzer component

operate on a computer and

receive one or more factory inputs that provide the description,

the factory inputs include at least one of

user input,

model inputs,

schemas,

formulas,

equations,

files,

maps, or

codes.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component utilizing, at the very least, user input, model inputs, files, maps, and codes) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes

recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 ***additionally recites*** the limitation that; "The tool of claim 3, wherein

the factory inputs are processed by

the analyzer component to generate the security outputs,

the security outputs including

at least one of

manuals,

documents,

schemas,

executables,

codes,

files,

e-mails,

recommendations,

topologies,

configurations,

application procedures,

parameters,

policies,

rules,

user procedures, or

user practices

that are employed

to facilitate security measures in

an automation system.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 ***additionally recites*** the limitation that; "The tool of claim 2, wherein

the interface component includes

at least one of

a display output having associated display objects and

at least one input

to facilitate operations with

the analyzer component,

the interface component is associated with

at least one of

an engine,

an application,

an editor tool,

a web browser, or

a web service.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

10. Claim 6 ***additionally recites*** the limitation that; "The tool of claim 5, wherein the display objects include

at least one of

configurable icons,

buttons,

sliders,

input boxes,

selection options,

menus, or

tabs,

the display objects having

multiple configurable

dimensions,

shapes,

colors,

text,

data and

sounds

to facilitate operations with

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack

template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

11. Claim 7 ***additionally recites*** the limitation that; "The tool of claim 5,

the at least one input includes

user commands from at least one of

a mouse,

a keyboard,

speech input,

a web site,

a remote web service,

a camera, or

video input

to affect operations of

the interface component and

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing

tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

12. Claim 8 ***additionally recites*** the limitation that; "The tool of claim 2, wherein

the description includes

a model of one or more industrial automation assets

to be protected and

associated network pathways

to access the one or more industrial automation assets.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of **factory assets** whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration

changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

13. Claim 9 ***additionally recites*** the limitation that; "The tool of claim 2, wherein

the description

includes at least one of

risk data or

cost data

that is employed by

the analyzer component

to determine suitable security measures.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model, clearly dealing with risk and effective cost insofar as network security per se is concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 13, this claim is the method claim for the system claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 14 ***additionally recites*** the limitation that; "The method of claim 13,

wherein generating the one or more security outputs includes

generating one or more security outputs that include

at least one of recommended

security components,

codes,

parameters,

settings,

related interconnection topologies,

connection configurations,

application procedures,

security policies,

rules,

user procedures, or

user practices.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template

information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

15. Claim 15 ***additionally recites*** the limitation that; "The method of claim 13, further comprising:

automatically deploying the one or more security outputs

to the industrial controller; and

utilizing the security outputs

to mitigate at least one of

unauthorized network access and

network attack.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

16. Claim 19 ***additionally*** recites the limitation that; "The system of claim 17, further comprising:

a scanner component that automatically interrogates

at least one of

the industrial controller,

the I/O device, or

the controlled device

at periodic intervals for security-related data [*figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

a validation component that automatically assesses security capabilities

of the at least one of

the industrial controller,

the I/O device, or

the controlled device

based upon a comparison of

the security-related data and

one or more predetermined security guidelines [*figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., a validation component ...) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*]; and

a security analysis tool that recommends

at least one network interconnection

to achieve a specified security goal [*figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes (i.e., ' security analysis tool ... recommends interconnection ... a specified security goal ') in the network to counter vulnerabilities as*

a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]

indicated by the predetermined security guidelines.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above.

17. Claim 20 ***additionally recites*** the limitation that; "The system of claim 19, wherein the security guidelines

are automatically determined.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

18. Claim 21 ***additionally recites*** the limitation that; "The system of claim 46, wherein the host-based component performs

vulnerability scanning and

auditing on devices, and

the network-based component performs

vulnerability scanning and

auditing on networks.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

19. Claim 23 ***additionally recites*** the limitation that; "The system of claim 21, wherein

at least one of

the host-based component or

the network-based component

at least one of

non-destructively maps a topology of

information technology (IT) and

industrial automation devices,

checks revisions and configurations,

checks user attributes, or

checks access control lists.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing of **factory assets** whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

20. Claim 25 ***additionally recites*** the limitation that; "The system of claim 17, wherein the security action includes at least one of

automatically correcting the security events,

automatically adjusting security parameters,

altering network traffic patterns,

adding security components,

removing security components,

triggering alarms,

automatically notifying entities about detected problems and concerns,

generating an error or log file,

generating a schema,

generating data to re-configure or re-route network connections,

updating a database, or

updating a remote site.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, such that as modified by the Townsend in view of Godwind teachings to an applied network configuration, deal with the actual use of the combination (i.e., the security action per se encompassing the various limitations of this claim; '… automatically correcting the security events … removing security components … generating data to re-configure or re-route network connections …'), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

21. Claim 45 ***additionally recites*** the limitation that; "The tool of claim 1,

the analyzer component is adapted for

partitioned security specification entry and

sign-off from various groups.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., the network partitioned security specification) and attack template (i.e., inclusive of authentication aspects, insofar as sign-on/sign-off, at the very least would be concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

22. Claim 46 ***additionally recites*** the limitation that; "The system of claim 19,

the scanner component and

the validation component

are at least one of

a host-based component or

a network-based component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., scanner component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

23. Claim 47 ***additionally recites*** the limitation that; "The system of claim 21,

at least one of

the host-based component or

the network-based component

at least one of

determines susceptibility to

common network-based attacks,

searches for

open Transmission Control Protocol/User Datagram Protocol (TCP/UDP)

ports,

scans for

vulnerable network services,

attempts to gain identity information about

end devices that relates to

hacker entry, or

performs vulnerability

scanning and

auditing

on

firewalls,

routers,

security devices, and

factory protocols.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

24. Claim 48 ***additionally*** recites the limitation that; "The system of claim 41, the validation component automatically installs

one or more security components

in response to the one or more vulnerabilities.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters corresponds to said parameters as part of the installation criteria of the security parameters/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

25. Claim 49 ***additionally*** recites the limitation that; "The system of claim 1, wherein the analyzer component further

performs an automated action that disables network requests

from at least one outside network

upon detecting that

the current pattern of the data traffic deviates

from the learned pattern

in excess of the acceptable deviation.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters ('… disables network requests … upon detecting … current pattern of the data traffic deviate …') corresponds to said parameters as part of the installation criteria ('… in excess of a threshold …' e.g., Godwin, ¶0071-0078) of the security parameters/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

26. Claim 50 ***additionally*** recites the limitation that; "The system of claim 12, wherein the at least one automated security event includes

at least disabling network attempts to access

the industrial controller.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters/events corresponds to said parameters/events as part of the installation criteria of the security parameters/events/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

27. Claim 51 ***additionally*** recites the limitation that; "The method of claim 12, wherein the monitoring communication of data comprises at least one of

monitoring a number of network requests

to or from the industrial controller

over a given time frame or

monitoring a type of request

to or from the industrial controller

during the training period.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., vulnerability scanner component, inclusive of monitored/scanned information comprising the packet information, that upon being stored/logged ('… monitoring a number of network requests …') is such that stored log lines/events represent time tagged events ('… over a given time frame …') that are descriptive of the communications event (i.e., port number; '… monitoring a type of request …') per se) computer system/network configuration/topology/attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

28. Claim 52 ***additionally*** recites the limitation that; "The tool of claim 1, wherein the one or more security outputs alter the data traffic between

the controller and

the at least one I/O device to restore the learned pattern.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make

configuration changes in the network to counter vulnerabilities (as a function of the risks and costs associated with the changes recommended), as modified by Townsend/Godwin insofar as the automated update of security parameters subsequently applied to remediation of the determined vulnerability ('... security outputs ... alter the data traffic between ... controller ...') for the industrial controller networked ('... at least one I/O device to restore the learned pattern ...') environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

Response to Amendment

29. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the learning component aspect of the claims (Applicant's arguments of 21 May 2010, p. 12-16), the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

Data acquisition, insofar as collecting, storing/logging scanned network events/information (i.e., effectively a predetermined model/template as stored for subsequent use/comparison) gathered via direct network communications means (e.g., network port scanning, etc.,) or user/client type interaction (e.g., GUI, computer serial/parallel/USB port I/O, etc.,) clearly constitute the system ' learning ' such that subsequent use/comparison for the purpose of controlling/feedback via policy interaction/enforcement as applied to the various network access control aspects of the Swiler et al in view of Townsend/Godwin teachings would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

30. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the I/O table component aspect of the claims (Applicant's arguments of 21 May 2010, p. 12-16), the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

The I/O table – insofar as is broadly phrased in the claim limitations, is just a data structure as simple as an I/O buffer for a GUI (e.g., 'X' for UNIX based systems (e.g., Swiler, col. 2,lines 3-67; UNIX, etc.,), MS Windows GUI environments, etc.,) or the I/O table data structures used for computer serial/parallel/USB port I/O, etc., (see above), insofar as computer systems of Swiler et al in view of Townsend/Godwin clearly encompass such configurations and would therefore the ' I/O table ' phrase would ***not*** *add a* ***patently distinct limitation,*** as *broadly interpreted by the examiner*; and the references would be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

31. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the security outputs aspect of the claims (Applicant's arguments of 21 May 2010, p. 12-16), the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

The security outputs as a function of learned pattern deviation has been discussed in previous office actions in the various forms that they were presented (i.e., claim 1 above), and the previous arguments are still considered valid and therefore the Swiler et al in view of

Townsend/Godwin teachings would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

32. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the ' determination as to whether a current pattern of data traffic deviates from a learned pattern … ' aspect of the claims (Applicant's arguments of 21 May 2010, p. 12-16), the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

Swiler et al in view of Townsend/Godwin does make a determination insofar as patterns generated effectively are patterns learned via acquisition (see 1st ***Response to Amendment*** paragraph above) that subsequently are compared to the (real time/online acquired) pattern(s) – again as discussed above for the 35 U.S.C. 103(a) rejection above, and actions taken upon predetermined policy enforcement criteria. Further, as far as Townsend silent on the determination aspect, the real time/online acquired as compared to predetermined/acquired communications information/patterns - insofar as modifying the Swiler teaching, is addressed in the reasons/motivation for combining above. Therefore the Swiler et al in view of Townsend/Godwin teachings would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

33. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the ' output that alters the data traffic … ' aspect of the claims (Applicant's

arguments of 21 May 2010, p. 12-16), the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

The security outputs as a function of learned pattern deviation has been discussed in previous office actions in the various forms that they were presented (i.e., claim 1 above), and the previous arguments are still considered valid and further, the altering aspect is clearly the feedback aspect of the Swiler et al in view of Townsend/Godwin teaching for network policy enforcement criteria (i.e., the determined by comparison policy changes as implemented – post determined/compared). Therefore the Swiler et al in view of Townsend/Godwin teachings would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

34. As per applicant's argument concerning the lack of teachings by Swiler et al in view of Townsend/Godwin of the ' manner of assessment on network access patterns … ' aspect of the claims (Applicant's arguments of 21 May 2010, p. 12-16), insofar as the Godwin reference is concerned, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

Godwin involves the aspect of automatic correction/response as applied to Swiler et al in view of Townsend insofar as the ' bringing into compliance ' is effectively the automated security output applied to access control as a function of updated security/network access control policy as taught by Swiler et al in view of Townsend (i.e., control via policy enforcement in the network communications between associated network node(s) involved), and therefore the Swiler et al in

view of Townsend/Godwin teachings would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

Conclusion

35. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad, can be reached at (571) 272-7884. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439